Replacement Pages for Claims 1-40

(CLEAN FORM)

1. A method for use in distributing access to a data item, comprising:

allowing multiple transfers between computers of a single instance of permission to gain access to an encrypted data item, the encrypted data item having paged subsets that are accessible a paged subset at a time using the same instance of permission for each paged subset, the transfers occurring across data connections and including a first transfer between a first computer and a second computer and a subsequent transfer between the second computer and a third computer, wherein at any one time only one computer retains the instance of permission and is able to use the instance of permission to gain access to a paged subset of the encrypted data item at a time.

2. The method of claim 1, further comprising:

using an encryption key to impede unauthorized access to the encrypted data item.

3. The method of claim 1, wherein at least one of the transfers of permission includes the transfer of a first encryption key.

4. The method of claim 3, further comprising:

using a second encryption key to encrypt the first encryption key prior to transfer.

B1

5. The method of claim 4, wherein the first encryption key includes a secret key and the second encryption key includes one of the keys in a public/private key set.

6. The method of claim 1, further comprising:

using highly secure circuitry to help ensure that at any one time only one of the computers retains and is able to use the instance.

7. The method of claim 6, wherein the highly secure circuitry includes a smartcard computer.

8. The method of claim 6, wherein the highly secure circuitry includes a de-encryptor.

9. The method of claim 6, further comprising:

storing an encryption key in the highly secure circuitry.

10. The method of claim 9, further comprising:

using the encryption key only within the highly secure circuitry.

11. The method of claim 1, further comprising:

determining whether a computer is authorized to receive the instance of permission to gain access to the encrypted data item.

12. The method of claim 1, further comprising:

according to an expiration time, rendering at least one of transfers temporary.

13. The method of claim 12, further comprising:

in the temporary transfer, transmitting a copy of an encryption key from a sender computer to a recipient computer, and, at the expiration time, erasing the copy of the encryption key from the recipient computer.

14. The method of claim 1, further comprising:

in one of the transfers, transmitting a copy of an encryption key from a sender computer to a recipient computer, and erasing the copy of the encryption key from the sender computer.

15. The method of claim 1, further comprising:

associating at least one of the transfers with a transfer of funds.

B1

16. The method of claim 1, further comprising:

distinguishing between different instances of permission to gain access to the encrypted data item.

17. The method of claim 1, wherein at least one of the computers includes a Web server computer.

18. The method of claim 1, wherein at least one of the computers includes a book viewing device.

19. The method of claim 18, wherein the book viewing device includes a viewing screen and data communications circuitry.

20. A method comprising:

in accordance with access distribution parameters that are specific to an encrypted data item and that were established by a first computer, transferring, across a data connection from a second computer to a third computer and independently of the first computer, permission to gain access to the encrypted data item, the encrypted data item having paged subsets that are accessible a paged subset at a time using the same permission for each paged subset, wherein the permission may be used to gain access to a paged subset of the encrypted data item at a time.

21. A method comprising:

impeding a change to the number of computers that are allowed to gain access to an encrypted data item, independently of data connection transfers between computers of permission to gain access to the encrypted data item, the encrypted data item having paged subsets that are accessible a paged subset at a time using the same permission for each paged subset, wherein the permission may be used to gain access to a paged subset of the encrypted data item at a time.

22. A method for use in distributing access to a data item, comprising:

providing a first computer with permission to gain access to an encrypted data item, the encrypted data item having paged subsets that are accessible a paged subset at a time using the same permission for each paged subset, wherein the permission may be used to gain access to a paged subset of the encrypted data item at a time;

providing the permission by data connection to a second computer and removing the permission from the first computer; and

providing the permission by data connection to a third computer and removing the permission from the second computer.

23. A method comprising:

rendering accountably fungible an instance of permission data that allows a computer to gain access to encrypted book data, the encrypted data item having paged subsets that are accessible a paged subset at a time using the same instance of permission for each paged subset, wherein the instance of permission data may be used to gain access to a paged subset of the encrypted book data at a time.

24. A method for use in distributing access to a book data item, comprising:

associating highly secure circuitry with a device that is able to send and receive access data that is necessary to gain access to an encrypted book data item, the encrypted book data item having paged subsets that are accessible a paged subset at a time using the same access data for each paged subset, wherein the access data may be used to gain access to a paged subset of the encrypted book data item at a time, the highly secure circuitry including a computer processor and a program memory and being able to help an unauthorized transfer of the access data from the device.

25. A method for use in distributing access to a book data item, comprising:

at a publisher computer, storing publisher permission data that allows a number A of end-user computers to gain access to an encrypted book data item;

based on the publisher permission data, providing a distributor computer with distributor permission data that allows a number B of end-user computers to gain access to the encrypted book data item;

changing the publisher permission data so that the publisher permission data allows only a number A-B of end-user computers to gain access to the encrypted book data item;

based on the distributor permission data, providing a retailer computer with retailer permission data that allows a number C of end-user computers to gain access to the encrypted book data item;

changing the distribution permission data so that the distributor permission data allows only a number B-C of end-user computers to gain access to the encrypted book data item;

based on the retailer permission data, providing an end-user computer with end-user permission data that allows 1 end-user computer to gain access to the encrypted book data item, the encrypted book data item having paged subsets that are accessible a paged subset at a time using the same end-user permission data for each paged subset, wherein the end-user permission data may be used to gain access to a paged subset of the encrypted book data item at a time; and

changing the retailer permission data so that the retailer permission data allows only a number C-1 of end-user computers to gain access to the encrypted book data item;

wherein number A-B is non-negative, number B-C is non-negative, and number C-1 is non-negative.

26. A system for use in distributing access to a data item, comprising:

data processing apparatus for allowing multiple transfers between computers of a single instance of permission to gain access to an encrypted data item, the encrypted data item having paged subsets that are accessible a paged subset at a time using the same instance of permission for each paged subset, the transfers occurring across data connections and including a first transfer between a first computer and a second computer and a subsequent transfer between the second computer and a third computer, wherein at any one time only one computer retains the instance of permission and is able to use the instance of permission to gain access to the encrypted data item, wherein the instance of permission may be used to gain access to a paged subset of the encrypted data item at a time.

27. A system comprising:

a transferor, in accordance with access distribution parameters that are specific to an encrypted data item and that were established by a first computer, transferring, across a data connection from a second computer to a third computer and independently of the first computer, permission to gain access to the encrypted data item, the encrypted data item having paged subsets that are accessible a paged subset at a time using the same permission for each paged subset, wherein the permission may be used to gain access to a paged subset of the encrypted data item at a time.

28. A system comprising:

an impedor impeding a change to the number of computers that are allowed to gain access to an encrypted data item, independently of data connection transfers between computers of permission to gain access to the encrypted data item, the encrypted data item having paged subsets that are accessible a paged subset at a time using the same permission for each paged subset, wherein the permission may be used to gain access to a paged subset of the encrypted data item at a time.

B1

29. A system for use in distributing access to a data item, comprising:

a first permission provider providing a first computer with permission to gain access to an encrypted data item, the encrypted data item having paged subsets that are accessible a paged subset at a time using the same permission for each paged subset, wherein the permission may be used to gain access to a paged subset of the encrypted data item at a time;

a second permission provider providing the permission by data connection to a second computer and removing the permission from the first computer; and

a third permission provider providing the permission by data connection to a third computer and removing the permission from the second computer.

30. A system comprising:

a renderor rendering accountably fungible an instance of permission data that allows a computer to gain access to encrypted book data, the encrypted book data having paged subsets that are accessible a paged subset at a time using the same instance of permission data for each paged subset, wherein the instance of permission data may be used to gain access to a paged subset of the encrypted book data at a time.

31. A system for use in distributing access to a book data item, comprising:

a device including highly secure circuitry, the device being able to send and receive access data that is necessary to gain access to an encrypted book data item, the encrypted book data having paged subsets that are accessible a paged subset at a time using the same access data for each paged subset, wherein the access data may be used to gain access to a paged subset of the encrypted book data item at a time, the highly secure circuitry including a computer processor and a program memory and being able to help prevent an unauthorized transfer of the access data from the device.

32. A system for use in distributing access to a book data item, comprising:

at a publisher computer, a storer for storing publisher permission data that allows a number A of end-user computers to gain access to an encrypted book data item;

a first permission provider for, based on the publisher permission data, providing a distributor computer with distributor permission data that allows a number B of end-user computers to gain access to the encrypted book data item;

a first permission changer for changing the publisher permission data so that the publisher permission data allows only a number A-B of end-user computers to gain access to the encrypted book data item;

a second permission provider for, based on the distributor permission data, providing a retailer computer with retailer permission data that allows a number C of end-user computers to gain access to the encrypted book data item;

a second changer for changing the distribution permission data so that the distributor permission data allows only a number B-C of end-user computers to gain access to the encrypted book data item;

a third permission provider for, based on the retailer permission data, providing an end-user computer with end-user permission data that allows 1 end-user computer to gain access to the encrypted book data item, the encrypted book data item having paged subsets that are accessible a paged subset at a time using the same end-user permission data for each paged subset, wherein the end-user permission data may be used to gain access to a paged subset of the encrypted book data item at a time; and

a third changer for changing the retailer permission data so that the retailer permission data allows only a number C-1 of end-user computers to gain access to the encrypted book data item;

wherein number A-B is non-negative, number B-C is non-negative, and number C-1 is non-negative.

33. Computer software, residing on a computer-readable medium, comprising instructions for use in distributing access to a data item, the instructions causing a computer to:

allow multiple transfers between computers of a single instance of permission to gain access to an encrypted data item, the encrypted data item having paged subsets that are accessible a paged subset at a time using the same instance of permission for each paged subset, the transfers occurring across data connections and including a first transfer between a first computer and a second computer and a subsequent transfer between the second computer and a third computer, wherein at any one time only one computer retains the instance of permission and is able to use the instance of permission to gain access to the encrypted data item, wherein the instance of permission may be used to gain access to a paged subset of the encrypted data item at a time.

34. Computer software, residing on a computer-readable medium, comprising instructions for causing a computer to:

in accordance with access distribution parameters that are specific to an encrypted data item and that were established by a first computer, transfer, across a data connection from a second computer to a third computer and independently of the first computer, permission to gain access to the encrypted data item, the encrypted data item having paged subsets that are accessible a paged subset at a time using the same permission for each paged subset, wherein the permission may be used to gain access to a paged subset of the encrypted data item at a time.

35. Computer software, residing on a computer-readable medium, comprising instructions for causing a computer to:

impede a change to the number of computers that are allowed to gain access to an encrypted data item, independently of data connection transfers between computers of permission to gain access to the encrypted data item, the encrypted data item having paged subsets that are accessible a paged subset at a time using the same permission for each paged subset, wherein the permission may be used to gain access to a paged subset of the encrypted data item at a time.

36. Computer software, residing on a computer-readable medium, comprising instructions for use in distributing access to a data item, the instructions causing a computer to:

provide a first computer with permission to gain access to an encrypted data item, the encrypted data item having paged subsets that are accessible a paged subset at a time using the same permission for each paged subset, wherein the permission may be used to gain access to a paged subset of the encrypted data item at a time;

provide the permission by data connection to a second computer and removing the permission from the first computer;

provide the permission by data connection to a third computer and removing the permission from the second computer.

37. Computer software, residing on a computer-readable medium, comprising instructions for causing a computer to:

render accountably fungible an instance of permission data that allows a computer to gain access to encrypted book data, the encrypted book data having paged subsets that are accessible a paged subset at a time using the same instance of permission data for each paged subset, wherein the instance of permission data may be used to gain access to a paged subset of the encrypted book data at a time.

38. Computer software, residing on a computer-readable medium, comprising instructions for use in distributing access to a book data item, the instructions causing a computer to:

associate highly secure circuitry with a device that is able to send and receive access data that is necessary to gain access to an encrypted book data item, the encrypted book data item having paged subsets that are accessible a paged subset at a time using the same access data for each paged subset, wherein the access data may be used to gain access to a paged subset of the encrypted book data item at a time, the highly secure circuitry including a computer processor and a program memory and being able to help an unauthorized transfer of the access data from the device.

39. Computer software, residing on a computer-readable medium, comprising instructions for use in distributing access to a book data item, the instructions causing a computer to:

at a publisher computer, store publisher permission data that allows a number A of end-user computers to gain access to an encrypted book data item;

based on the publisher permission data, provide a distributor computer with distributor permission data that allows a number B of end-user computers to gain access to the encrypted book data item;

change the publisher permission data so that the publisher permission data allows only a number A-B of end-user computers to gain access to the encrypted book data item;

based on the distributor permission data, provide a retailer computer with retailer permission data that allows a number C of end-user computers to gain access to the encrypted book data item;

change the distribution permission data so that the distributor permission data allows only a number B-C of end-user computers to gain access to the encrypted book data item;

based on the retailer permission data, provide an end-user computer with end-user permission data that allows 1 end-user computer to gain access to the encrypted book data item, the encrypted book data item having paged subsets that are accessible a paged subset at a time using the same end-user permission data for each paged subset, wherein the end-user permission data may be used to gain access to a paged subset of the encrypted book data item at a time; and

B1

change the retailer permission data so that the retailer permission data allows only a number C-1 of end-user computers to gain access to the encrypted book data item;

wherein number A-B is non-negative, number B-C is non-negative, and number C-1 is non-negative.

40. A method for use in distributing access to a data item, comprising:

allowing multiple transfers between computers of a single instance of permission to gain access to an encrypted book data item, the encrypted book data item having pages that are accessible a page at a time using the same instance of permission for each page, the transfers occurring across data connections and including a first transfer between a first computer and a second computer and a subsequent transfer between the second computer and a third computer, wherein at any one time only one computer retains the instance of permission and is able to use the instance of permission to gain access to a page of the encrypted book data item at a time for display purposes.